CLAIMS

1. A key management mechanism comprising:

an IP-key for entering a closed IP network;

a key generator for generating from the IP-key a set of session keys indexed for identification, the set of session keys having a divergence barrier incorporated therein for barring a computational approach to an arbitrary session key;

an index pointer for pointing an index to identify a session key; and

an unbar data set for unbarring the divergence barrier.

2. The key management mechanism of claim 1, wherein:

an arbitrary pair of session keys are information-theoretically isolated from each other by a drop of information therebetween having an entropy difference corresponding thereto; and

the divergence barrier develops as an integrated entropy difference along a way of the computational approach.

3. The key management mechanism of claim 2, wherein the unbar date set defines the drop of information between the arbitrary pair of session keys.

4. The key management mechanism of claim 2, wherein the drop of information comprises a lost data on one of a sign data and a numeral data of a respective session key.

5. The key management mechanism of claim 1, wherein:

the divergence barrier comprises a tree of candidate keys for the arbitrary session key; and

the tree of candidate keys diverge with an increasing number of candidate keys beyond a computationally secure number, as the computational approach makes a way.

6. The key management mechanism of claim 5, wherein the unbar data set defines a unique candidate key to be the arbitrary session key.

7. The key management mechanism of claim 1, wherein the unbar data set comprises a regenerated set of session keys, and a sequence of index combinations for identifying a unique session key in the regenerated set of session keys.

8. The key management mechanism of claim 7, wherein:

the regenerated set of session keys comprises a sequence of boxes of session keys; and

a respective index combination comprises a combination of a first index for identifying a unique box of session keys, and a second index for identifying the unique session key in the unique box of session keys.

9. The key management mechanism of claim 1, wherein the index pointer does not point the index of any session key more than one time.

10. The key management mechanism of claim 1, wherein part of the unbar data set is built in an outer IP header and transmitted as a cleartext on the closed IP-network to a communication peer for a connection-less mission of a key agreement in an IP layer of the closed IP network.

09547078.100300